Право. Журнал Высшей школы экономики,
2014, №1, С. 129-139
Опубликована: Янв. 2, 2014

Безопасность информации при использовании облачных сервисов органами государственной власти

Терещенко Людмила Константиновна

Заместитель заведующего отделом административного законодательства и процесса Института законодательства и сравнительного правоведения при Правительстве Российской Федерации, доктор юридических наук, Заслуженный юрист Российской Федерации. Адрес: 117134, Российская Федерация, г. Москва, ул. Большая Черемушкинская, д. 34. E-mail: adm2@izak.ru

Аннотация

В статье рассматриваются проблемы, связанные с использованием «облачных» технологий в сфере государственного управления. Пока «облачные» технологии используются в нашей стране недостаточно активно, но отчетливо просматривается тенденция на расширение сферы их применения. Приняты программные документы, в которых предусмотрено создание национальных платформ «облачных» сервисов. В настоящее время в основном используются «облачные» услуги иностранных провайдеров, что вызывает ряд вопросов, связанных с информационной безопасностью и возможностью их использования в деятельности государственных и муниципальных органов. Приводится анализ действующего законодательства с точки зрения наличия или отсутствия существующих ограничений использования облачных технологий в сфере государственного управления. Автор приходит к вводу, что действующим законодательством не установлены прямые запреты применительно к возможности использования «облачных» технологий, однако запреты и ограничения могут быть связаны с видом информации: государственная тайна, конфиденциальная информация, различные виды тайн, а также с обязательством сторон о получении письменного согласия другой стороны на передачу информации третьей стороне. Таким образом, на допустимость использования облачных сервисов российскими государственными и муниципальными органами, иными организациями с государственным и муниципальным участием может оказывать влияние характер обрабатываемой информации и установленный в отношении нее правовой режим.

Ключевые слова: информационная безопасность, облачные технологии, органы государственной власти, услуг, провайдер,

ограничение использования, облачных, трансграничная передача данных

Использование облачных технологий опосредуется несколькими видами договоров с разной степенью контроля за обрабатываемой и хранимой в «облаках» информацией, что оказывает влияние на решение вопроса о возможности использования «облаков». Одна из основных причин, по которой «облачные» вычисления могут быть ограничены в использовании, связана, в первую очередь, с передачей ряда функций «облачному» провайдеру и, как следствие, потерей контроля за собственными данными. Пользователь не всегда имеет достаточную и достоверную информацию, чтобы оценить безопасность используемых провайдером «облачных» технологий, гарантии сохранности своей информации, а также обеспечить контроль за соблюдением установленного режима информации.

В России все шире распространяется применение «облачных» технологий. 20 октября 2010 г. было принято распоряжение Правительства Российской Федерации N° 1815-р «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)»[1]. В подпрограмме «Информационное государство» в рамках развития электронного правительства предусмотрено создание национальной платформы «облачных вычислений». Включение в государственную программу позиции, предусматривающей создание национальной платформы «облачных вычислений» в рамках развития электронного правительства, свидетельствует о том, что указанные технологии будут активно внедряться в сферу государственного и муниципального управления.

Однако каких-либо пояснений относительно того, что имеется в виду под «облачными вычислениями», в программе нет. Нет и четкого представления, что представляют собой «облачные вычисления» с позиции права. Учитывая, что предполагается оказывать услуги на базе облачных технологий органам государственной власти, бизнесу и гражданам, одного только упоминания «облачных вычислений» недостаточно. В связи с этим представляется важным определить, что понимается под «облачными вычислениями», как они «вписываются» в правовое поле и нуждается ли действующее законодательство в корректировке, чтобы облачные технологии могли активно использоваться не только гражданами и коммерческими организациями, но и государственными и муниципальными структурами в их практической повседневной деятельности.

1. СЗ РФ. 2010. № 46. Ст. 6026.

Если в английском языке рассматриваемому явлению соответствует только один термин — «cloud computing», то в русском языке используются несколько близких по значению терминов; облачные технологии, облачные (рассеянные) вычисления, облачные сервисы, облачная (рассеянная) обработка данных. Все приведенные русскоязычные термины означают технологию распределенной обработки данных, в которой компьютерные ресурсы и мощности предоставляются пользователю через сеть Интернет как интернет-сервис. Именно распределенная обработка данных позволяет говорить о «рассеянной» технологии.

Термин «облачные вычисления» часто на практике используется для обозначения любых услуг, которые предоставляются через сеть Интернет, хотя, на наш взгляд, это расширительное понимание «облачных вычислений». В настоящее время существующую совокупность «облачных сервисов» принято разделять на три основные категории, которые, в свою очередь, могут подразделяться на более мелкие группы:

- инфраструктура как сервис;
- платформа как сервис;
- программное обеспечение как сервис.

«Облачные» вычисления обладают как привлекательными возможностями, так и недостатками, которые связаны, в первую очередь, с передачей ряда функций «облачному» провайдеру и, как следствие, потерей контроля за собственными данными. Основная причина, по которой «облачные» вычисления могут быть ограничены в использовании, связана, в первую очередь, с передачей ряда функций по обработке информации «облачному» провайдеру. Пользователь зачастую не имеет достаточной и достоверной информации, чтобы оценить безопасность используемых провайдером «облачных» технологий, гарантии сохранности своей информации. Он только имеет доступ к собственным данным и возможность работы с ними.

Вместе с тем облачные технологии — это то, что уже применяется и будет применяться еще шире в ближайшем будущем. В распоряжении Правительства Российской Федерации от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)»[2] говорится о создании национальной платформы

«облачных вычислений». Однако на сегодняшний день основной объем «облачных» услуг оказывается с использованием зарубежных «облаков».

В связи с этим возникает вопрос о допустимости использования облачных сервисов российскими государственными и муниципальными органами, иными организациями с государственным и муниципальным участием с учетом принадлежности «облаков». При этом важно не только наличие (или отсутствие) прямых запретов по использованию облачных сервисов, но и вид и характер информации, которые могут прямо или косвенно влиять на возможность использования таких сервисов и условий такого использования, а также функции государственных и муниципальных органов, которые могут быть переданы «облачному» провайдеру.

Прямого ограничения применения облачных технологий на уровне федеральных законов нет. Однако на допустимость использования облачных сервисов российскими государственными и муниципальными органами, иными организациями с государственным и муниципальным участием может оказывать влияние характер обрабатываемой информации и установленный в отношении нее правовой режим. В отношении одних категорий информации государство должно обеспечить защиту от неправомерного доступа и использования третьими лицами, а в отношении других, напротив, обеспечить доступность и препятствовать закреплению прав или установлению каких-либо ограничений.

Применительно к сведениям, не предназначенным для широкого круга лиц (различные виды тайн, информация конфиденциального характера), всегда установлено ограничение доступа, использования и распространения, а нарушение установленных в отношении этих сведений требований может повлечь отрицательные последствия. Использование облачных технологий опосредуется несколькими видами договоров с разной степенью контроля за обрабатываемой и хранимой в «облаках» информацией, что оказывает влияние на решение вопроса о возможности использования облачных технологий.

Что касается информации государственных и муниципальных структур, то они обязаны обеспечить сохранность информации ограниченного доступа и исключить возможность несанкционированного доступа, модификации, распространения и т.д.

2. СЗ РФ. 2010. № 46. Ст. 6026.

Важным с этой точки зрения является постановление Правительства Российской Федерации от 18.05.2009 г. № 424 «Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям». Указанное постановление Правительства Российской Федерации устанавливает обязанности операторов федеральных государственных информационных систем, которые влияют на возможность применения облачных вычислений в целом и, облачных сервисов иностранного провайдера, в частности:

- обеспечение защиты информации, содержащейся в информационных системах общего пользования, от уничтожения, изменения и блокирования доступа к ней;
- обеспечение постоянного контроля возможности доступа неограниченного круга лиц к информационным системам общего пользования;
- обеспечение восстановления информации, измененной или уничтоженной вследствие несанкционированного доступа к ней, в течение не более восьми часов;
- использование при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям средств защиты информации, прошедших оценку соответствия (в том числе, в установленных случаях сертификацию), в порядке, установленном законодательством Российской Федерации;
- обеспечение информационной безопасности при подключении информационных систем общего пользования к информационно-телекоммуникационным сетям.

Указанные обязанности основаны на нормах Указа Президента Российской Федерации[3], который устанавливает, что

- подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации,

3. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети Интернет не допускается;

- при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российская Федерация порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;
- государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;
- размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего

эксплуатацию таких технических средств в указанных помещениях.

Указанные положения значительно осложняют использование облачных услуг, которые предоставляются иностранными провайдерами, поскольку налагают па них дополнительные требования по необходимости установки средств защиты информации, в том числе, шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю, а также налагают запрет на подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации.

Кроме того, оператор облачного сервиса также должен выполнять требования по обеспечению безопасности информации в информационных системах, созданных с использованием суперкомпьютерных и грид-технологий, установленные Федеральной службой по техническому и экспортному контролю (подл, «г» п. 3 Указа Президента Российской Федерации от 8 февраля 2012 г. № 146 «О федеральных органах исполнительной власти, уполномоченных в области обеспечения безопасности информации в информационных системах, созданных с использованием суперкомпьютерных и грид-технологий»).

Отдельно следует сказать, что нормативные правовые акты устанавливают ограничения в отношении отдельных видов информации, которые вообще не подлежат размещению в информационных сетях общего доступа, что также влияет на возможности использования «облачных технологий». Так, постановлением правительства Российской Федерации от 25 сентября 2012 г. № 1775-р утвержден Перечень товаров, работ, услуг в сфере использования атомной энергии, сведения о закупках которых не составляют государственную тайну, но не подлежат размещению на официальном сайте.

Постановление Правительства Российской Федерации от 20 августа 2013 г. N° 719 «О государственной информационной системе государственного надзора в сфере образования» указывается, что вносимая в государственную информационную систему информация не должна содержать сведения, составляющие государственную или иную охраняемую законом тайну. При этом органы государственной власти обеспечивают полноту, достоверность и актуальность вносимой ими в информационную систему информации, а также конфиденциальность и безопасность содержащихся в ней персональных данных, соблюдение требований законодательства Российской Федерации о государственной или иной охраняемой законом тайне.

Ограничение размещения в информационных системах информации, доступ к которой ограничен законодательством Российской Федерации об информации, информационных технологиях и о защите информации, о государственной тайне, о коммерческой и иной охраняемой законом тайне, регламентировано постановлениями Правительства Российской Федерации: 1) от 9 августа 2013 г. № 681 «О государственном экологическом мониторинге (государственном мониторинге окружающей среды) и государственном фонде данных государственного экологического мониторинга (государственного мониторинга окружающей среды)»; 2) от 10 июля 2013 г. N° 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети Интернет в форме открытых данных»; 3) от 2 сентября 2010 г. № 671 «О порядке формирования государственного задания в отношении федеральных государственных учреждений и финансового обеспечения выполнения государственного задания»; 4) от 4 февраля 2013 г. № 80 «Об утверждении Положения о порядке доступа к информации, содержащейся в государственной информационной системе топливно-энергетического комплекса» и др.

Обеспечение конфиденциальности информации, а следовательно и особый порядок ее защиты является непременным условием государственных контрактов[4]. Такое условие предусматривает, что сведения, относящиеся к предмету государственного контракта, ходу его исполнения и полученным результатам предназначены исключительно для сторон и не

могут быть полностью (частично) переданы (опубликованы, разглашены) третьим лицам или использованы каким-либо иным способом с участием третьих лиц без согласия сторон.

Вместе с тем следует отметить, что типы «облаков» могут быть разными, а сами «облака» существенно отличаться друг от друга, в том числе в позиции безопасности. Таким образом, степень безопасности «облака» и возможность контроля за безопасностью информации — это основные критерии, па основании которых можно принимать решения об использовании облачных технологий.

Некоторые документы, определяющие развитие тех или иных сфер, затрагивают вопросы применения облачных технологий, однако, как правило, регламентация отношений в этих документах отсутствует. В Концепции создания единой информационной системы в сфере здравоохранения и программах модернизации здравоохранения па 2011-2012 годы, утвержденной приказом Минздравсоцразвития от 28 апреля 2011 г. № 364[5], «облачная» модель принята в качестве базовой, однако имеются в виду государственные национальные «облака».

Федеральная целевая программа «Развитие судебной системы России на 2013-2020 годы», утвержденная постановлением Правительства Российской Федерации от 27 декабря 2012 г. N° 1406, в целях развития информационных технологий в судебной системе предполагает, в частности, реализацию мероприятий по созданию «облачной» вычислительной архитектуры, которая позволит максимально эффективно, надежно и безопасно использовать технологии и специализированное «облачное» программное обеспечение для автоматизации судебного и общего делопроизводства. В рамках этого мероприятия планируется разработка единой «облачной» системы автоматизации судопроизводства и электронного документооборота, создание главного центра обработки данных, а также создание 10 центров обработки данных в федеральных арбитражных судах округов. Решение этих задач позволит реализовать возможность удаленного доступа как со стороны

4. См., напр.: постановление Правительства Российской Федерации от 23 января 2004 г. № 41 «Об утверждении примерных государственных контрактов на выполнение научно-исследовательских и опытно-конструкторских работ по государственному оборонному заказа»; постановление Правительства Российской Федерации от 31 октября 2009 г. № 880 «Об утверждении примерных форм договоров о передаче прав на единые технологии и примерной формы договора о выполнении дополнительных работ по доведению единой технологии до стадии практического применения с учетом потребностей заинтересованного лица» и т.д.

5. Бюллетень трудового и социального законодательства Российской Федерации. 2011. № 7.

судов, так и со стороны участников судебных процессов из любой точки страны и мира и с любого устройства, в том числе мобильного. Каких-либо ограничений к облачному провайдеру документ не содержит, но сама программа предполагает создание государственного облака.

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и па перспективу до 2025 года, утвержденная распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, также предусматривает наличие национальной «облачной» среды. В ней будут размещены для органов государственной власти и государственных организаций наиболее популярные сервисы массового потребления с учетом достаточных мер безопасности при сохранении эргономики использования.

Предполагается также совершенствование процессов сбора и обработки ведомственной статистической информации, обеспечение поэтапного перехода от использования форм отчетности федерального и регионального уровней к автоматизированным процессам учета и обработки статистических показателей на основе «облачных» технологий и сервисов.

Развитие облачных решений является основной тенденцией российского рынка детских информационных технологий и медиа (распоряжение Правительства Российской Федерации от 11 июня 2013 г. № 962-р «Об утверждении Стратегии развития индустрии детских товаров на период до 2020 года и плана первоочередных мероприятий на 2013-2015 годы по ее реализации»). Динамичное развитие информационного общества, внедрение информационных технологий в сферу оказания публичных услуг гражданам и субъектам предпринимательской деятельности, формирование электронного правительства обуславливает применение возможностей «облачных» технологий в указанной области.

Хранение и обработка информации посредством платформы «облачных вычислений» является одним из мероприятий:

- по дальнейшему развитию электронного правительства (распоряжение Правительства Российской Федерации от 20 октября 2010 г. №1815-р «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)», Указ Президента от 21 августа 2012 г. № 1202 «Об утверждении Положения об Управлении Президента Российской Федерации по применению

информационных технологий и развитию электронной демократии»);

- при проектировании и разработке «электронного бюджета» (распоряжение Правительства Российской Федерации от 20 июня 2011 г. N° 1275-р «О Концепции создания и развития государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет»). Посредством виртуального сервера предусматривается доступ к открытой части электронного бюджета.

Однако применение «облачных вычислений» в рассматриваемой области ограничивается двумя факторами:

- созданием национальной платформы «облачных вычислений»;
- необходимостью обеспечения необходимого уровня отказоустойчивости и катастрофоустойчивости[6].

Последнее свойство облачного сервера не раскрывается, однако явно свидетельствует об обязанности оператора «облака» сохранять возможность контроля за хранением и обработкой передаваемой в «облако» информацией. Создание национальной платформы «облачных вычислений» предполагает отказ от услуг иностранных провайдеров.

Применение сервисов для предоставления возможностей по использованию географически распределенных суперкомпьютерных ресурсов и уникального оборудования («облачных вычислений») предусматривается и в сфере биотехнологий в качестве одного из мероприятия системы информационно-аналитического обеспечения программных мероприятий (Комплексная программа развития биотехнологий в Российской Федерации на период до 2020 года, утвержденная Правительством Российской Федерации 24 апреля 2012 г, N° 1853п-П8).

Следует выделить и еще два направления, в которых актами Правительства Российской Федерации предусматривается применение грид-технологий и «облачных вычислений»:

- развитие информационной базы регионов.

6. См.: распоряжение Правительства Российской Федерации от 4 марта 2013 г. № 293-р «Об утверждении государственной программы Российской Федерации «Управление государственными финансами».

- развитие информационно-коммуникационных технологий и систем, стратегических компьютерных технологий и программ, как результат совместной деятельности организаций, участвующих в пилотном проекте по созданию национального исследовательского центра «Курчатовский институт».

При решении вопроса о возможности использования «облачных» вычислений следует учитывать принятые Федеральной службой по техническому и экспортному контролю (ФСТЭК РФ) нормативные правовые акты, в частности, Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (приказ ФСТЭК России от 11 февраля 2013 г. № 17), и Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (приказ ФСТЭК России от 18 февраля 2013 г. N° 21).

Пункт 7 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, устанавливает, что защита информации, содержащейся в государственной информационной системе, обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе. Следует учесть, что требования, утвержденные ФСТЭК России, распространяют свое действие на обладателей информации, заказчиков, заключивших государственный контракт па создание государственной информационной и операторов государственных информационных систем.

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее — уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. При этом, как указывается в Требованиях, в договоре должна быть предусмотрена обязанность

уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с требованиями ФСТЭК России.

При определении состава мер защиты информации и их базовых наборов для соответствующего класса защищенности информационной системы, которая содержит информацию, не относящуюся к государственной тайне, в приказе ФСТЭК России от 11 февраля 2013 г. N” 17 используется понятие «контролируемой зоны», под которой понимается зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования. При этом доступ в контролируемую зону лиц, не уполномоченных на обработку содержащейся в информационной системе информации, должен быть либо ограничен (система пропусков, контроль за пребыванием и т.д.), либо запрещен[7].

Таким образом, прямых запретов на использование облачных технологий российским законодательством не установлено, а сферы деятельности, в которых могут быть использованы облачные услуги, не ограничиваются. Более того, их использование возможно, однако в ряде случаев требуется соблюдение установленных процедур и требований, что может оказаться затруднительным. Тем самым необходимость выполнения установленных процедур и требований может повлечь ограничение использования облачных технологий, что связано с обеспечением должной степени защиты от несанкционированного доступа к ней, искажению, изменению и неразглашению.

Библиография

1. Указ Президента Российской Федерации от 17. марта 2008 г № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационнотелекоммуникационных сетей международного информационного обмена» // СЗ РФ. 24 марта 2008 г. №12. Ст. 1110.

7. Так, в приказе Минкомсвязи России от 27 декабря 2013 г. № 190 «Об утверждении Технических требований к взаимодействию информационных систем в единой системе межведомственного электронного взаимодействия» устанавливается, что доступ посторонних лиц ко всем техническим средствам системы взаимодействия, каналам связи и поддерживающим системам (электропитания, вентиляции, кондиционирования и т.п.) в контролируемой зоне участника взаимодействия должен быть исключен.

2. Постановление Правительства Российской Федерации от 20 августа 2013 г. № 719 «О государственной информационной системе государственного надзора в сфере образования» // СЗ РФ. 26 августа 2013 г. № 34. Ст. 4448.
3. Постановление Правительства Российской Федерации от 9 августа 2013 г. № 681 «О государственном Экологическом Мониторинге ((осударственном Мониторинге Окружающей Среды) и государственном Фонде Данных государственного Экологического Мониторинга (Государственного Мониторинга Окружающей Среды)» // СЗ РФ. 19 августа 2013 г. № 33. Ст. 4383.
4. Постановление Правительства Российской Федерации от 10 июля 2013 г. № 583 «Об обеспечении доступа к общедоступной информации о деятельности государственных органов и органов местного самоуправления в информационно-телекоммуникационной сети Интернет в форме открытых данных» //СЗ РФ. 29 июля 2013 г. № 30 (ч. II). Ст. 4107.
5. Постановление Правительства Российской Федерации от 2 сентября 2010 г. № 671 «О порядке формирования государственного задания в отношении федеральных государственных учреждений и финансового обеспечения выполнения государственного задания» // СЗ РФ. 13 сентября 2010 г. № 37. Ст. 4686.
6. Постановление Правительства Российской Федерации от 4 февраля 2013 г. № 80 «Об утверждении Положения о порядке доступа к информации, содержащейся в государственной информационной системе топливно-энергетического комплекса» // СЗ РФ. 11 февраля 2013 г. № 6. Ст. 560
7. Распоряжение Правительства Российской Федерации № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы) // СЗ РФ. 2010. № 46. Ст. 6026.
8. Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011-2020 годы)» // СЗ РФ. 2010. № 46. Ст. 6026.
9. Концепция создания единой информационной системы в сфере здравоохранения и программах модернизации

здравоохранения на 2011-2012 годы, утверждена приказом Минздравсоцразвития от 28 апреля 2011 г. № 364 // Бюллетень трудового и социального законодательства РФ. 2011. №7.